Multi-National Information Sharing

Cross Domain Collaborative Information Environment (CDCIE) Solution

United States Joint Forces Command
Joint Futures Lab

Mr. Boyd Fletcher (boyd.fletcher@je.jfcom.mil)
Mr. Dana Hare (dana.hare@je.jfcom.mil)

12 April 2005
Revision 4

ABSTRACT

In February 2004, the Joint Forces Command (JFCOM) began its efforts to provide a near term Multinational Information Sharing (MNIS) solution to support Warfighters operating in a coalition environment. The JFCOM Joint Futures Laboratory (JFL) solution to MNIS is the Cross Domain Collaborative Information Environment (CDCIE). The CDCIE is a suite of standards-based and largely open source code applications that provide the capability to collaborate, share and manage documents, and use web portals, from one classification domain to another. The applications will also work within a single classification domain. While the CDCIE is designed to run in today's environment, it is also a building block for the future information infrastructure – the CDCIE is adhering to the same basic standards that are guiding Net-Centric Enterprise Services development.

Currently portal, document management, and cross domain text chat capabilities have been developed for the CDCIE solution. The cross domain text chat capability will be submitted for Certification and Accreditation (C&A) this year. CDCIE development will continue to be expanded to include audio chat, application casting and whiteboarding. As the CDCIE is enhanced, the suite will return to C&A. The CDCIE project has been designed to function at the operational command and control level.

INTRODUCTION

In the future, United States military operations will include coalition partners. To be effective, the Department of Defense (DoD) community must share mutually beneficial information with all of the coalition partners. Member nations and non-governmental organizations of U.S. led coalitions will present a wide range of security classification and releasability problems to U.S. Military operations. These security problems will have a profound effect on the levels of information sharing possible in coalition operations. There are two fundamental aspects of this coalition information sharing problem:

1. How do you share information within a single classification domain with coalition partners?
2. How do you share information between classification domains?

In the past, the Department of Defense (DoD) has focused on point solutions for both problems. This has led to multiple systems that are non-interoperable, frequently proprietary, and expensive to procure, train on, and maintain. Joint Forces Command (JFCOM) has worked for the past year to develop a single solution to solve both parts of the MNIS challenge. The result of JFCOM's Joint Futures Lab (JFL) development efforts is the Cross Domain Collaborative Information Environment (CDCIE) prototype. The goal of the CDCIE project is to develop a fieldable and accreditable prototype to provide a standards based, largely open source, secure, scalable collaborative information environment to enable cost-effective multinational information sharing (MNIS) in both single and cross domain environments. The CDCIE project has been designed to function at the operational command and control level (for information classified Secret GENSER and below).

JFCOM is actively engaged with people at the following organizations for its MNIS development process: National Security Agency (NSA), Defense Integration Systems Agency (DISA), MNIS Executive Agent, and Air Force Research Lab (AFRL in Rome, NY). Other contributors include Old Dominion University, Space and Naval Warfare (SPAWAR) SC San Diego, Trident Systems, DigitalNet (now BAE Systems), MITRE, Xythos Inc., eXo Platform SARL, Sun Microsystems, OpenOffice.org, and North Atlantic Treaty Organization (NATO) Allied Command for Transformation (ACT).

DISCUSSION

The CDCIE project consists of five parts:

1. *Cross Domain Portal and Portal Applications* which provide a portal and suite of commonly used portal applications.
2. *Cross Domain Document Management System* which provides an easy to use system for securely sharing documents with versioning and subscription support and a method to automate much of the Reviewer/Releaser process.
3. *Cross Domain Collaborative Tool* which provides a secure and scalable collaboration tool for DoD that solves the tactical chat and cross domain collaboration requirements

4. *Security Enhanced Office Automation Suite* which provides a method to safely release documents to lower classification levels and external entities and enhances the automation of the Reviewer/Releaser process.
5. *Cross Domain XML Guard* which provides a high performance, memory and socket based XML Guard.

This paper will cover the Requirements, Standards, Architecture, Design, and Security aspects of the CDCIE effort.

Requirements and Standards

CDCIE's near term functional requirements are to provide an integrated solution to identified MNIS problems. These requirements include:

- DJC2 Baseline Requirements
- COCOM cross domain information sharing requirements
- GRIFFIN and CENTRIXS information sharing requirements
- OIF Information Sharing Lessons Learned
- Tactical Chat requirements for the DoD
- Reviewer/Releaser process efficiency requirements

The CDCIE project also developed a set of technical requirements on which a framework could be developed for a workable long term solution. The technical requirements include the following goals:

- Work toward the Global Information Grid (GIG)/Net Centric Enterprise Services (NCES) vision
- Promote next generation standards and develop new ones where they are lacking
- Maximize Benefits of Open Standards and Open Source software and processes to Stimulate industry participation and give Coalition partners the ability to roll their own interoperable solutions
- Reduce the cost of collaboration in DoD

Standard protocols and development practices were selected to meet the functional and technical requirements. These are listed below for each of the major areas.

Portal, Document Management, and Portal Applications (called Portlets)

- Hardware, Database, and Operating System independence using Java
- Enterprise-class Architecture using Java2 Enterprise Edition 1.4
- Standards based portal applications. Compliance with the Java Specification Request for Portlet APIs (JSR-168) (Portlet API) and Web Services for Remote Portals (WSRP)
- Portlet based access to system-of-record situational awareness data via web services including the ability to interoperate with GCCS, GCSS, TBMCS, and NCES web services

- Flexible portal layout engine with support for unlimited number of rows, columns, and tabs
- Modern design patterns used including Inversion of Control (IoC) and Model-View-Controller (MVC)
- User configurable preferences which support a robust set of group layout/page controls
- Ability for the portal to be configured based on roles and user groups
- High scalability with an ability to support 500 connections per second to the portal server (a four CPU Pentium 4 server)
- Document Management System with versioning and subscription notification support that is fully Web Distributed Authoring and Versioning (WebDAV) compliant
- WebDAV Searching and Locating using DASL
- Enhanced versioning over WebDAV using DeltaV
- Support for drag-and-drop access to files and directories in the document management system including support for Microsoft's client side implementation of WebDAV (sometimes called Web Folders)
- Integrated content and metadata search engine of both documents and portlet data
- Granular control of permissions on documents and folders including the ability to set *read*, *write*, *delete* and *administrate* permissions with full permission inheritance
- Support for Lightweight Directory Access Protocol (LDAP) version 3 and Active Directory for user authentication and authorization
- Portal Standards using Java Specification Request for Portlet APIs (JSR-168) (Portlet API) and Web Services for Remote Portals (WSRP)

Security:

- Advanced Encryption Standard (AES) for all encryption
- Transport Layer Security (TLS) (FIPS Compliance capable version of SSL) for TCP/IP encryption; Client side PKI verifies the sender identity
- eXtensible Markup Language (XML) for the cross domain file format and portlet data.
- XML Digital Signature (XML-DSIG) and XML Encryption specifications from the World Wide Web consortium to sign and encrypt XMPP messages

Security Enhanced Office Automation Suite (SE OAS):

- XML based Open Office File Format from OASIS as the file format for all documents transferring across the XML Guard

Real Time Collaboration Tool:

- eXtensible Messaging and Presence Protocol (XMPP), also known as Jabber, from the Internet Engineering Task Force (IETF) for one-to-one text chat, multi-user chat, publish-subscribe (PubSub), delivering alerts, delivering the whiteboard, and providing the signaling for the audio and application casting streams
- XML based OASIS Common Alerting Protocol (CAP) sent over XMPP for all message alerts; a portlet is used to send the alerts to the clients

- XML based Scalable Vector Graphics (SVG) specification from the World Wide Web consortium as the basis of the white boarding protocol; white boarding protocol uses XMPP and its PubSub extension
- Portable Network Graphics (PNG) specification from the World Wide Web consortium for encoding the images for application casting protocol (which is sent over RTP) and the white board's presentation mode
- Secure Real-Time Transport Protocol (SRTP) to provide the transport for the audio and application casting session
- Patent-free open source Speex audio codex to provide high quality speech over a wide range of bandwidths

CDCIE Architecture

The CDCIE high-level architecture is shown in Figure 1. It consists of a portal, a document management system, and two collaboration servers supported by a database, cross domain collaborative gateway, and a cross domain XML guard. The core enabler for the cross domain data transfer is a high-performance, low latency, socket and memory-based XML guard. The cross domain design strategy is to turn most information streams into carefully marked and tagged XML and to use the XML guard to transfer the data between classification domains. The portal and document management system can be run on multiple servers and load-balanced using a TCP/IP load balancer for increased scalability and fault tolerance. The XMPP servers and RTP server can be distributed in a loosely connected mesh configuration similar to SMTP based email server configurations. The following sections discuss each of the architecture components.

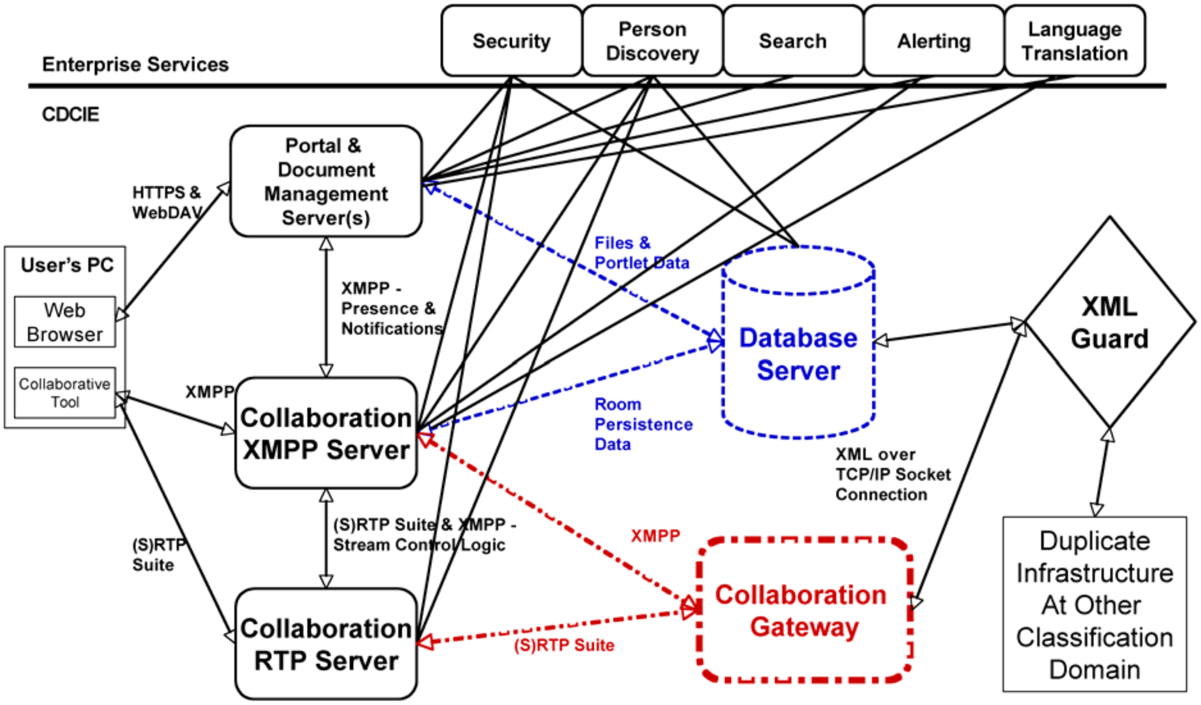

Figure 1 - CDCIE High-Level Architecture

Portal Server

The CDCIE Portal is based on the commercial open source eXo Portal. This portal was one of the first certified JSR-168 portals, and supports the Web Services for Remote Portlets (WSRP) specification. The selection of the J2EE, JSR-168, and WSRP standards enabled JFCOM to develop portal applications, a search engine infrastructure, and presence/notification engine that are portable across any fully compliant JSR-168 portal and J2EE application server. When running in a cross domain mode of operation, the portal and portal applications (called portlets) use Oracle's Label Security feature to safely tag data of different classifications. Classification labeling and data tagging are key security features to enable MNIS. When operating in single domain mode, a variety of databases are supported including Oracle, Postgres, and SQL Server. eXo has several other features that made it the choice as the portal for CDCIE to include:

- A very flexible layout engine with good group layout/page controls
- Use of modern Java design patterns including Inversion of Control (IoC) and Model-View-Controller (MVC) pattern
- Support for the development of Web Services using WSRP producers and consumers and SOAP. It can be used as an enabler for a Service Oriented Architecture
- Low cost - essentially free as long as eXo specific applications are not developed and support is not needed. eXo is dual licensed under both the GNU Public License (GPL) license and a commercial license (consultation with an organization's legal office is suggested to determine which license is suitable)
- Support for Windows, Linux, Solaris, and Mac OS X server operating systems

- Ability to work with all modern web browsers including Internet Explorer, Netscape, Mozilla, FireFox, Safari, and Opera with no loss in functionality
- Support for server load balancing
- Support to integration with the JBoss J2EE engine

The heart of any Portal system is the applications or portlets that provide functionality to the user. Below is a list of commonly used portal applications that have been developed for the CDCIE. eXo also includes a number of portlets for things like iFrames and Rich Site Summary (RSS) feeds. The initial set of non-military specific portal applications includes the following:

- Document Management Portlet
- News Portlet
- Group Calendar Portlet (can feed Outlook via iCal)
- Bookmarks/Hyperlinks Portlet
- Subject Matter Expert (SME) Locator Portlet
- White/Yellow Pages Portlet
- What you see is what you get (WYSIWYG) Notepad (Message) Portlet
- Image Portlet
- Banner Portlet
- Table/Form Generator w/ charting
- Help Desk Portlet
- Message Alert System Management Portlet
- Scrolling Marquee
- Roles Management Portlet
- Subscription Management Portlet
- Discussion Forum Portlet
- Collaboration Tool Management Portlets

The initial set of military-specific portal applications developed by JFL includes the following:

- Security Information Portlet;
- Request for Information (RFI)/Knowledge Request (KR) Portlet;
- Fragmentary order (FRAGO) Workflow Portlet;
- Convoy Tracker;
- Chief of Staff Tasker Tracker.

In a traditional portal environment, portal applications generally lack the ability to tag data with classification labels. In the CDCIE, applicable portal applications have been extended to support classification labeling. If enabled in an application, classification labeling is handled by the use of Hibernate interceptors. During the cross domain transfer process, Oracle Label Security is used to prevent application programmatic errors from causing an inadvertent release of non-releasable information. The cross domain transfer process extracts the releasable data from the database and generates an XML file that is sent to the XML Guard for transfer across domain.

Document Management Server

Xythos is a commercial document management system based on the J2EE and WebDAV standards. It supports the all the major databases (Postgres, Oracle and MS SQL Server), and all the major operating systems (Windows, Linux, Solaris, and MacOS X). It also works with all modern web browsers including Internet Explorer, Netscape, Mozilla, FireFox, Safari, and Opera web browsers). Xythos also supports server load balancing.

JFCOM has developed a JSR-168 compliant portlet that exposes Xythos in the portal. The portlet requires that all files uploaded into the document management system be labeled with a classification label. It is not possible (without a custom client being installed) to prompt a WebDAV session (like MS Web Folders) to enter a classification label on file copy operations, so an event listener for Xythos has been written that intercepts all files written to the server via WebDAV and sets their classification label the system high level. The cross domain file process enforces a two step method to release documents for transfer. First, a document must be properly labeled with a classification label and must be securely saved in the Open Office file format. Second, a user in the *release* administrative role is required to download the document, visually verify its releasability, digitally sign the document, upload the signed document back to the portal, and then check the release button for the document. Prior to the transfer occurring, the portal verifies the file is properly labeled, that the database and file have the same label, that it has been digitally signed by both the author and the *release* administrator, that secure save has been run, and that it is of the proper type (Open Office File Format). If a document fails any of these checks, its release is rejected and an error notification is sent to the information assurance staff.

Collaboration Tool

The collaborative tool will provide instant messaging, presence awareness, group text chat, white boarding, presentations, language translation, audio, and application casting. eXtensible Messaging and Presence Protocol (XMPP) was chosen as the core communication protocol used by the tool. XMPP is a pure XML streaming protocol defined by the IETF Request for Comment (RFC)s 3920 and 3921. It is currently listed as an emerging standard in the DoD IT Standards Registry (DISR - the replacement for the Joint Technical Architecture). The CDCIE project is currently using the following XMPP Servers:

- Coversant SoapBox Server 2005 SR-1 for Windows installations
- Jabber Inc. XCP 4.0 for Unix/Linux installations
- Jive Messenger (modified) for the Collaboration Gateway

The collaborative tool is a heavily modified version of BuddySpace, an open source Java XMPP client from the Open University in the UK. Currently implemented capabilities for BuddySpace include the following:

- Presence awareness - allows a user to see the online status of other users
- Instant messaging - one way asynchronous messaging capability analogous to email (except that it is not persistent)
- One-to-one chat - interactive chat session with one other user

- Group text chat - interactive chat with any number of other users. Group text chat supports the notion of roles and associated permissions
- Content filtering alerts - capability to identify a set of key words or phrases to monitor for in selected group chat rooms
- Hyper-Room - single window interface to multiple group chat sessions. This provides an easy way to simultaneously monitor text chat in different group chat sessions
- Full multi-user chat support
- Classification labeling using the Intelligence Community [IC] Metadata Standard for Classification Labeling
- XML Encryption
- XML Digital Signatures
- Bi-directional language translation using CyberTrans II

Future additions to the collaborative tool include white boarding, presentations, audio, and application casting. The white boarding feature will use the XML based Scalable Vector Graphics (SVG) to describe white board objects. The presentations feature will provide the capability to send a PowerPoint slideshow to other users in the Portal Network Graphic (PNG) format. CDCIE uses the NSA developed CyberTrans II language translation middleware. This Java based middleware provide a common web services based interface to a wide variety of commercial and government developed language translation engines. The chat client supports automatic inbound and outbound translation and language pivoting (uses an intermediary language to provide a pairing between the source and destination languages).

When operating in cross domain mode, the collaborative tool uses the Collaboration Gateway (CG) from AFRL and Trident Systems to provide an XMPP front-end to the XML guard. The Collaboration Gateway provides the following features:

- Authentication which authenticates a client when it requests access to the Cross Domain services
- Authorization which checks if a given user is authorized to access a resource, either a multi-user chat room or one-to-one chat. It generates a shared symmetrical encryption key that can be used to bootstrap other group services, i.e. data security
- Data Security which guarantees that a sender of the message can be uniquely identified
- Confidentiality which guarantees that no member outside the group may gain access to session content (including chat server)
- Integrity which guarantees that any modification of a message is detectable by a receiver
- Group authenticity which guarantees that a message was delivered by a member of the group
- Logging which provides audit trail of all cross-domain chat sessions

Security Enhanced Office Automation Suite

Historically, the most frequently requested cross domain transfer feature is the ability to move files across classification domains. While this process is relatively simple and systems have been in place for years that securely transfer files, these systems suffer from a common flaw – they do not have the ability to validate the contents of all the files types they can transfer. Of particular concern are Microsoft Office documents. The Microsoft Office file format is used heavily in DoD and coalition environments, but present several challenges: it is proprietary, poorly understood, and has a number of features that can make transfer of documents across classification domains extremely risky. The Security Enhanced Office Automation Suite (SE OAS) attempts these solve the problems by implementing a secure save mechanism and an XML file format while still maintaining the ability to read and write MS Office documents.

The SE OAS uses version 2.0 of the open source Open Office product from Sun Microsystems and the OpenOffice.org community. The security enhancement functionality:

- Strips revision history and track changes from documents
- Strips "deleted" text from documents
- Strips scripting and macros from documents
- Strips binary data including images and embedded objects from documents
- Requires that documents be properly labeled including title pages and classification labels on each page
- Eliminates invisible text remediation (text color same (or near) as background)
- Digitally signs the document using the user's and reviewer's PKI certificates
- Provides the capability to create and modify text documents, spreadsheets and presentations that are compatible with Microsoft Office
- Uses a native XML based file format (OASIS's Open Office file format)

In addition to the security enhancements, SE OAS is supported on MS Windows, Linux, Solaris, and Mac OS X operating systems. The SE OAS is integrated into the reviewer/release process that has been implemented in the document management system.

Cross Domain Guard

Early in the initial design process for CDCIE, JFCOM decided to use XML as the data format for moving information between classification domains. With the exception of images (in application casting, presentations and documents) and collaboration audio data, all information transiting the guard is in XML. XML was chosen because of the rich parsers available, industry support, and the ability to describe (XML Schema), verify (XML Schema) and transform XML documents (XML Stylesheets). No production XML guards were available at the start of the project, however several were under development. After examining the guards under development, JFCOM decided to fund some significant performance and parsing improvements to the XML based Data Sync Guard from BAE Systems (formally DigitalNet). This guard is based STOP/OS 6.1.E, which is BAE System's EAL 5+ evaluated operating system. It runs on their XTS-400 Pentium 4 based platform. The guard supports a Linux API and uses the Xerces XML parser.

SUMMARY

Currently the portal, document management, and cross domain text chat capabilities of the CDCIE have been developed for the MNIS solution. The single domain version of the portal, document management system, and chat client has been fielded to Multi-National Force Iraq. The Portal and Document Management solution is currently being deployed as the US Joint Force Command portal.

The cross domain text chat including AFRL/Trident System's Collaboration Gateway and the BAE Systems Data Sync Guard will enter the Certification and Accreditation (C&A) process in early August 2005 for evaluation for connection between Secret and below networks.

REFERENCES

Organizations

- Apache Software Foundation (www.apache.org)
- DoD Joint Interoperability Test Command (jitc.fhu.disa.mil)
- International Standards Organization (www.iso.org)
- Internet Engineering Task Force (www.ietf.org)
- Jabber Software Foundation (www.jabber.org)
- Java Community Process (www.jcp.org)
- National Information Assurance Partnership (niap.nist.gov)
- National Institute for Standards and Technology (www.nist.gov)
- Organization for the Advancement of Structured Information Standards (www.oasis-open.org)
- SIP Forum (www.sipforum.org)
- Workflow Management Coalition (www.wfmc.org)
- World Wide Web Consortium (www.w3.org)

Web Sites

- Xythos
    - http://www.xythos.com
- eXo
    - http://www.exoplatform.com
- SVG
    - http://www.w3.org/Graphics/SVG
    - http://xml.apache.org/batik
- WebDAV
    - http://www.webdav.org
    - http://www.ietf.org/html.charters/webdav-charter.html
- XMPP/Jabber
    - http://www.jabber.org
    - http://www.ietf.org/html.charters/xmpp-charter.html
    - http://www.jabberstudio.org
- (S)RTP
    - http://www.ietf.org/iesg/1rfc_index.txt (search for RTP)
    - http://developer.apple.com/darwin/projects/streaming
    - http://srtp.sourceforge.net/srtp.html
- SASL
    - http://asg.web.cmu.edu/sasl
- SAML
    - http://shibboleth.internet2.edu
    - http:/www.opensaml.org
- HTML, XML, WSRP, Open Office File Format

  - http://www.w3.org
  - http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=office
  - http://www.openoffice.org
- Speex
  - http://www.speex.org
  - http://sourceforge.net/projects/jspeex
- Mozilla
  - http://www.mozilla.org
- JSR-168 and JSR-147
  - http://www.jcp.org/en/jsr/detail?id=168